Accellion Share Securely™

AN ACCELLION WHITE PAPER

8 Critical Requirements for Secure, Mobile File Sharing and Collaboration

Accellion, Inc.
1804 Embarcadero Road
Suite 200
Palo Alto, CA 94303

Tel +1 650 485-4300
Fax +1 650 485-4308
www.accellion.com
info@accellion.com

Executive Summary

As mobile devices such as smartphones and tablets become increasingly popular, business users are coming to expect 24/7 mobile access to business data and tools. By giving users mobile access to secure collaboration and file sharing, enterprises can boost business productivity and organizational agility. But enterprises must ensure that mobile file sharing never jeopardizes data security or regulatory compliance.

This white paper describes the requirements—such as server-based security, data encryption, and audit trails—that secure file sharing solutions must meet in order to deliver mobile access while protecting data confidentiality and regulatory compliance.

Why Businesses Need Secure File Transfer and Collaboration with Mobile Access

Enterprises are more geographically distributed than ever before, and the pace of business gets faster every day. Online collaboration has become a business necessity—there's no other way for distributed teams to work as quickly and efficiently as business demands.

Users are embracing this fast pace of work and the "anytime, anywhere" model of data access that goes with it. They're accessing email, file sharing, and other collaboration services from almost any device, especially iPads, which few enterprises have authorized for use. And they're accessing this data from all kinds of locations, including home offices, client offices, coffee shops, airports, and public parks.

Determined to make data access as fast and easy as possible, business users are also signing up for dropbox-type file sharing services, without the knowledge or approval of their IT departments. The services are usually inexpensive or free, so no purchase-authorization process is necessary. A minute filling out a web form, the click of a Submit button, and users are online, sharing business data with colleagues and other users, as well.

Unfortunately, these "free," convenient services are dangerous: they pose serious data security and compliance risks for the enterprise. Designed originally for home users or small businesses, these services typically lack enterprise-grade security features such as role-based access controls, data encryption, and audit logs. Enterprises need these features—and others, as well—in order to protect confidential data, to prevent data breaches, and to ensure compliance with industry regulations such as SOX and HIPAA.

Mobile access makes meeting these security requirements all the more difficult. A secure file sharing solution must be able to work with the wide variety of mobile devices that business users are carrying, including personal devices owned by employees, as well as business devices tested and configured by the IT department. Many users carry multiple devices—for example, a BlackBerry issued by the IT department, along with an iPad for personal use. A secure file sharing solution must be able to support all these devices without requiring the enterprise to hire an army of technicians to install and maintain special security software on every mobile device that might potentially access enterprise servers.

How can enterprises ensure that, no matter what mobile devices employees are using, they have secure, auditable access to business data and vital collaboration tools they need? How can they make mobile access to secure collaboration an extension of IT infrastructure, rather than an operational encumbrance?

8 Critical Requirements for Secure File Sharing with Mobile Access

A successful deployment of mobile access for enterprise collaboration involves security, usability, availability, and integration. Enterprises should evaluate mobile-access solutions for compliance with the following requirements.

1. **Provides server-based security.**
   Enterprises should select a solution that relies on server-based security, rather than client-based security, so IT doesn't face the impossible task of configuring an ever-changing collection of hundreds or thousands of mobile devices, including personal smartphones. Server-based security also enables administrators to enforce changes to security policies immediately. For example, to disable mobile access for an ex-employee, they don't have to get hold of that person's mobile phone; they can simply turn off access through an administrative dashboard.

2. **Limits data access to authorized users.**
   The collaboration solution should prevent unauthorized users from accessing confidential data. The solution should also enforce different levels of access rights based on a user's role in a project. For example, some users need to be able to create workspaces, while others need to be able to both read and write files, and other users need only to read files, not edit or create them. Data security policies might include preventing administrators from reading confidential data in workspaces. Administrators need access to controls for account creation and activity monitoring, but in most cases they should not need to be given unfettered access to business data. Another data security best practice is offering users the ability to set expiration dates on files. Expiration dates enable authorized users to access data within a reasonable amount of time, while ensuring that sensitive data is not stored on servers indefinitely.

3. **Supports internal and external users.**
   Employees need to collaborate not only with colleagues but also with external users, such as business consultants, ad agencies, industrial design firms, legal counsel, and other types of business partners. Employees need a secure collaboration solution that works with all team members working on a project, including external users, without access to the internal network domain. The solution should support cross-boundary collaboration, so mobile users can work with all members of a team, including external users.

4. **Encrypts data in transit and at rest.**
   The solution should apply advanced encryption algorithms such as AES 128-bit or AES 256-bit encryption, to protect data at rest and in transit. Hackers should never be able to intercept or tamper with confidential data.

5. **So easy to use, users are not tempted to seek work-arounds.**
   Mobile apps should have an intuitive interface and be available for common mobile platforms, such as Android, Apple iOS, and BlackBerry. When security solutions are easy-to-use, employees use them, rather than looking for work-arounds that might put confidential data at risk.

6. **Integrates with the IT infrastructure people already use.**
   The solution should integrate easily with an enterprise's existing IT infrastructure, including LDAP directories, Active Directory services, archiving systems, and data loss prevention (DLP) systems. Integration with directories ensures that access controls are consistently enforced across all IT services. Integration with archiving and DLP systems enables collaboration services to be part of broader data security initiatives and practices. And, of course, a secure file transfer and collaboration solution should integrate with current investments in solutions such as Microsoft® SharePoint®, Microsoft® OCS, and Autonomy® iManage®.

7. **Monitors data access and maintains an audit trail.**
   The solution should support logging and audit features, so IT can monitor system usage and so the enterprise can comply with industry regulations such as SOX and HIPAA that require monitoring and reporting systems to be in place.

8. **Supports system configurations that deliver the highest possible availability.**
   The solution's architecture should readily accommodate fail-over configurations with stand-by servers, ensuring that if a system outage occurs, users still have continuous access to the data they need.

Accellion Mobile Apps

Accellion provides enterprise-class secure collaboration and managed file transfer solutions that enable professionals to share information and collaborate freely, while securing confidential data and ensuring regulatory compliance.

With native Accellion Mobile Apps, employees can share files and collaborate securely from mobile devices. Accellion Mobile Apps give authorized mobile users secure access to files in Accellion Secure Workspaces. Mobile users can browse workspaces, share files, subscribe to notifications, and post comments.

Accellion offers native applications for Apple iOS, BlackBerry, and Android mobile devices. Using these apps' intuitive user interface, business users can quickly, easily, and securely access files in an Accellion Secure Workspace from any location. Accellion makes sharing files–whether proposals, contracts, engineering specs, architectural designs, or content on an upcoming advertising campaign–easy and secure. Mobile access to secure collaboration increases business productivity and employee responsiveness.

Because Accellion Mobile Apps use patented Accellion secure file sharing technology, enterprises and government agencies can be assured that sensitive or confidential information, intellectual property, and customer data is protected both in transit and at rest. Enterprises can offer secure collaboration with mobile access while demonstrating compliance with industry regulations such as HIPAA, GLBA and SOX.

Accellion Mobile Apps work with Accellion Secure Collaboration, a secure collaboration platform that makes it easy for enterprise users to share information with internal and external parties while securing confidential data and ensuring regulatory compliance. Accellion Secure Collaboration integrates with LDAP directories and other key pieces of enterprise IT infrastructure. It features the logging and audit trail capabilities required for compliance with regulations like HIPAA. To ensure that users have continual access to their secure workspaces, the platform supports fail-over configurations with stand-by servers.

Together, Accellion Secure Collaboration and Accellion Mobile Apps meet the security, usability, availability, and compatibility requirements of an effective mobile access solution for secure collaboration.

Conclusion

Extending collaboration services to mobile users can be a great boon to productivity and business agility—but enterprises can never afford to have mobile services jeopardize IT security or regulatory compliance.

Accellion Mobile Apps offer enterprises a proven security solution for giving employees and other trusted users mobile access to the collaboration services they need.

For more information, please visit www.accellion.com.

